AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Missouri

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* INFORMATION ASSOCIATED WITH DISCORD ACCOUNT HUNGOBJECT#3945 (USER ID 730942504312111125) THAT IS STORED AT PREMISES CONTROLLED BY DISCORD, INC., 444 DE HARO ST., SUITE 200, SAN FRANCISCO, CA 94107	Case No. 4:22 MJ 3067 NCC SIGNED AND SUBMITTED TO THE COURT FOR FILING BY RELIABLE ELECTRONIC MEANS

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

SEE ATTACHMENT A

located in the NORTHERN District of CALIFORNIA, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. Sections 875(d), 2251, 2252, 2252A, 2261A(2)(b) and/or 2422	Interstate transmission of threat to injure property or reputation with intent to extort; Sexual exploitation of children; stalking; Use of mail or any facility or means of foreign/interstate commerce to coerce/entice a person under 18 to engage in prostitution or any criminal sex act

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

I state under the penalty of perjury that the foregoing is true and correct.

Applicant's signature

Derek G. Velazco, Special Agent, FBI

Printed name and title

Sworn to, attested to, or affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41.

Date: 3/9/2022

Judge's signature

City and state: St. Louis, MO

Honorable Noelle C. Collins, U.S. Magistrate Judge

Printed name and title

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH DISCORD ACCOUNT **HUNGOBJECT#3945 (USER ID 730942504312111125)** THAT IS STORED AT PREMISES CONTROLLED BY DISCORD, INC., 444 DE HARO ST., SUITE 200, SAN FRANCISCO, CA 94107	)	No. 4:22 MJ 3067 NCC FILED UNDER SEAL

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Derek G. Velazco, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) and Federal Criminal Procedure 41 for information associated with [a] certain account[s] that is stored at premises controlled by **Discord, Inc.** a social media and communication provider headquartered at 444 De Haro Street, San Francisco, CA 94107 (hereinafter referred to as "the Provider"). The information to be searched is described in the following paragraphs and in Attachment A. The search warrant would require the Provider to disclose to the United States copies of the information (including the content of communications) further described in Attachment B. Upon receipt of the information described in Section I of Attachment B, United States-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I, Derek G. Velazco, am a Special Agent with the Federal Bureau of Investigation (FBI) in the St. Louis Division. I have been an FBI agent since March 2017. Additionally, I have been employed with the FBI for a total of 15 years, having served in several administrative and

analytical roles prior to becoming a Special Agent. In the course of my duties, I have investigated both criminal and national security matters for my agency and in partnership with various other criminal investigative and intelligence agencies. These investigations have included terrorism and counterintelligence; however, the majority of my investigations have been related to violent crimes committed against children or human trafficking. I have received and provided training matters related to violent crimes against children and human trafficking.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 875(d), 2251, 2252, 2252A, 2261A(2)(b), and/or 2422, have been committed by Gerardo Montes and/or other persons yet to be determined. There is also probable cause to search the location described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

LOCATION TO BE SEARCHED

5. The location to be searched is:

HUNGOBJECT#3945 (USER ID 730942504312111125) (hereinafter referred to as the "Subject Account") located at 444 De Haro Street, San Francisco, CA 94107, further described in Attachment A. The items to be reviewed and seized are described in Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

DEFINITIONS

7. The following definitions apply to this Affidavit and Attachments A and B to this Affidavit:

a. The term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such a device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device. 18 USC § 1030(e).

b. The term "minor" means any individual under the age of 18 years. 18 USC § 2256(1).

c. "Sexually explicit conduct" means actual or simulated sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibition of the anus, genitals, or pubic area of any person. 18 USC § 2256(2)(A).

d. "Visual depiction" includes undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image. 18 USC § 2256(5).

e. "Child pornography" includes any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct or such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct. 18 USC § 2256(8)(A) or (C).

f. "Identifiable minor" means a person who was a minor at the time the visual depiction was created, adapted, or modified; or whose image as a minor was used in creating, adapting, or modifying the visual depiction; and who is recognizable as an actual person by the person's face, likeness, or other distinguishing characteristic, such as a unique birthmark or other recognizable feature; and shall not be construed to require proof of the actual identity of the identifiable minor. 18 USC § 2256(9).

g. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software or digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

h. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade

form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (compact discs, electronic or magnetic storage devices, hard disks, CD-ROMs, DVDs, Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), thumb drives, flash drives, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, electronic notebooks, cellular telephones, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

i. Electronic data may be more fully described as any information stored in the form of electronic, magnetic, optical, or other coding on computer media or on media capable of being read by a computer or computer-related equipment.

j. "Child erotica" are materials or items that are sexually arousing to pedophiles but that are not in and of themselves obscene or which do not necessarily depict minors in sexually explicit poses or positions.

k. “IP address” refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might be static whereby the user’s ISP assigns his computer a unique IP address – and that same number is used by the user every time his computer accesses the Internet. Numerical IP addresses generally have corresponding domain names. For instance, the IP address 149.101.10.40 traces to the corresponding domain name “www.cybercrime.gov”. The Domain Name System or DNS is an Internet service that maps domain names. This mapping function is performed by DNS servers

located throughout the Internet. In general, a registered domain name should resolve to a numerical IP address.

l. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, genital-anal, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals or pubic area of any person.

CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

8. Most individuals who collect child pornography are sexually attracted to children, as their sexual arousal patterns and erotic imagery focus, in part or in whole, on children. The collection may be exclusively dedicated to children of a particular age/gender or it may be more diverse, representing a variety of sexual preferences involving children. Collectors of child pornography express their attraction to children through the collection of sexually explicit materials involving children, as well as other seemingly innocuous material related to children.

9. The above-described individuals may derive sexual gratification from actual physical contact with children, as well as from fantasy involving the use of pictures or other visual depictions of children or from literature describing sexual contact with children. The overriding motivation for the collection of child pornography may be to define, fuel, and validate the collector's most cherished sexual fantasies involving children.

10. Visual depictions may range from fully clothed depictions of children engaged in non-sexual activity to nude or partially nude depictions of children engaged in explicit sexual activity. In addition to child pornography, these individuals are also highly likely to collect other paraphernalia related to their sexual interest in children. This other material is sometimes referred to as "child erotica," further defined as any material relating to children that serves a sexual purpose

for a given individual. "Child erotica" is broader and more encompassing than child pornography, though at the same time the possession of such corroborative material, depending on the context in which it is found, may be behaviorally consistent with the offender's orientation toward children and indicative of his/her intent. “Child Erotica” includes things such as fantasy writings, letters, diaries, books, sexual aids, souvenirs, toys, costumes, drawings, cartoons and non-sexually explicit visual images.

11. Child pornography collectors often reinforce their fantasies by taking progressive, overt steps aimed at turning such fantasy(ies) into reality in some, or all, of the following ways: collecting and organizing their child-related material; masturbating while viewing child pornography; engaging children, online and elsewhere, in conversations, sometimes sexually explicit conversations, to fuel and fortify the fantasy; interacting, both directly and indirectly, with other like-minded adults through membership in organizations catering to their sexual preference for children, thereby providing a sense of acceptance and validation within a community; gravitating to employment, activities and/or relationships which provide access or proximity to children; and frequently persisting in the criminal conduct even when they have reason to believe the conduct has come to the attention of law enforcement. These are need driven behaviors to which the offender is willing to devote considerable time, money, and energy in spite of risks and contrary to self-interest.

12. Child pornography collectors almost always maintain and possess their material(s) in the privacy and security of their homes or some other secure location, to include Internet cloud storage, such as Dropbox, Box, and Google cloud storage. The collection may include sexually explicit or suggestive materials involving children, such as photographs, magazines, narratives, motion pictures, video tapes, books, slides, drawings, computer images or other visual media. The

collector is often aroused while viewing the collection and, acting on that arousal, he/she often masturbates, thereby fueling and reinforcing his/her attraction to children.

13. Due to the fact that the collection reveals the otherwise private sexual desires and intent of the collector and represents his most cherished sexual fantasies, the collector rarely disposes of the collection. The collection may be culled and refined over time, but the size of the collection tends to increase. Individuals who use a collection in the seduction of children or to document the seduction of children treat the materials as prized possessions and are especially unlikely to part with them. Even if a child pornography collector deletes files from his hard drive or other electronic media, a computer expert is often able to retrieve those files using computer forensic tools.

BACKGROUND CONCERNING DISCORD

14. Discord, Inc., (the "Provider") is an instant messaging and digital distribution platform that allows users to communicate with voice calls, video calls, text messaging. Users can also share media and other files in private chats or in group chats.

15. In my training and experience, I have learned that the Provider provides a variety of on-line services to the public. The Provider allows subscribers to obtain social media and/or communication accounts similar to the one listed in Attachment A. Subscribers obtain an account by registering with the Provider. During the registration process, the Provider asks subscribers to provide basic personal information. Therefore, the computers of the Provider are likely to contain stored electronic communications (including retrieved and unretrieved email for the Provider subscribers) and information concerning subscribers and their use of the Provider services, such as account access information, message transaction information, and account application information. In my training and experience, such information may constitute evidence of the

crimes under investigation because the information can be used to identify the account's user or users.

16. Subscribers can also store with the Provider files in addition to messages, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by the Provider. In my training and experience, evidence of who was using an account may be found in address books, contact or buddy lists, communication messages in the account, and attachments to communications, including pictures and files.

17. In my training and experience, social media providers generally ask their subscribers to provide certain personal identifying information when registering for an account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

18. In my training and experience, social media account providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage

of the account. In addition, providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

19. In my training and experience, in some cases, account users will communicate directly with a service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

20. As explained herein, information stored in connection with an account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, messages, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the provider can show how and when the account was accessed or used. For example, as described below, providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time

and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

PROBABLE CAUSE

21. On or about January 14, 2022, the FBI received an anonymous tip through the FBI National Threat Operations Center regarding F.W., who is a 14-year-old minor female. The tip came from an IP address which resolved to Hoshangābād, Madhya Pradesh (India). Based on the affiant's investigative experience, it is possible that the IP's location was the result of a virtual private network (VPN). This report was documented in the FBI's Guardian system and routed to the St. Louis Division for investigation.

22. The tip claimed that F.W., with a provided reddit link, is being blackmailed by Hungobject (https://www.reddit.com/user/Hungobject) to send him explicit pictures otherwise he will spread naked pictures of her that he obtained elsewhere online. The tip further stated that the latest blackmail message came at 1:00 PM Newburg, Missouri time. Finally, the tip stated that he (Hungobject) is fully aware of F.W.'s age yet he continues to ask for sexually explicit images.

23. On or about January 20, 2022, the report was assigned to your affiant for investigation. On or about that same day, your affiant conducted open-source research and determined that F.W. is a minor female in Newburg, Missouri, within the Eastern District of Missouri, who struggled with self-mutilation and suicidal ideation.

24. On or about January 21, 2022, your affiant, along with other representatives from the FBI and local law enforcement, responded to F.W.'s residence in Newburg, Missouri. At this time, your affiant spoke with F.W. who confirmed that nude images of her had been exchanged with "hungobject" on both Discord and Reddit. F.W. claimed that she originally believed that the user of this account was 21-years-old, but later found out that he is 31-years-old. In compliance with FBI policy, your affiant paused further questioning of the victim until such time a child forensic interviewer could conduct a more specified interview.

25. On or about January 24, 2022, an administrative subpoena was sent to Reddit requesting information related to username "hungobject."

26. On or about January 27, 2022, Reddit responded to the administrative subpoena and stated that the user account "hungobject" was registered on or about September 7, 2018, and is associated with email address giminiking00@hotmail.com.

27. On February 9, 2022, FBI analytic personnel searched the email address giminiking00@hotmail.com via open-source search tools. This search provided a potential user, Gerardo Montes, as well as additional email addresses associated with Montes. These email addresses included giminiking99@yahoo.com and hungobject@hotmail.com.

28. A LexisNexis Comprehensive Report dated February 2, 2022, shows that Montes is a 31-year-old male who resides in an apartment in Honolulu, Hawaii. The report further shows

that Montes is associated with email addresses hungobject@hotmail.com and giminiking99@yahoo.com.

29. Open-source searches for Montes located a LinkedIn page (https://www.linkedincom/in/gerardo-montes-1146a0171). This page included an image of Montes in which a tattoo is partially visible on his left forearm. Additionally, the page stated that Montes worked as "Admin/HR Support Assistant at The Research Corporation of the University of Hawai'i".

30. On February 22, 2022, F.W. participated in a child abuse forensic interview with an FBI forensic interviewer. During the interview, F.W. made several disclosures about the subject. F.W. stated she knew the subject as "hungobject" and stated she met the subject on a Reddit website. During the course of their communication, which lasted approximately two days, the subject disclosed that he was 31 years old, lived in Hawaii, and that he lived in an apartment. During the forensic interview of F.W., F.W. disclosed that "hungobject" was aware that she was 14 years of age.

31. During the course of the communications between F.W. and "hungobject," the subject requested a "boob" picture, which F.W. provided. Additionally, "hungobject" also requested the victim take additional photos where her top was removed, and her hair covered her breasts. F.W. complied and sent two additional images depicting this request. These images were full-body shots taken with F.W.'s Chromebook computer. In these images, F.W. was wearing pajama pants.

32. According to F.W., these images were screenshotted by "Hungobject." "Hungobject" then requested F.W. create five additional images. The images requested in specific in nature and requested: an image of F.W. nude on a couch with her legs spread; an image of F.W.

in the shower with "soap and bubbles"; a close-up photograph of F.W.'s "pussy"; an image of F.W. in a "doggie-style" position; and an additional image which F.W. did not recall.

33. "Hungobject" also sent nude images of another female to F.W. Based on the appearance of the female in the image, F.W. believed this female to be approximately 20 years old. "Hungobject" told F.W. that the female in the images was a former girlfriend.

34. F.W. refused to create these images as requested by "hungobject".

35. Later, F.W. was notified by another online associate that the images had been publicly posted via Discord.

36. During the forensic interview, F.W. was shown an image of Montes from his LinkedIn page. F.W. stated that she did not know what "hungobject" looked like. However, after seeing the image, F.W. stated "hungobject" had a tattoo on his forearm.

37. An administrative subpoena was sent to the Provider for information related to accounts associated with giminiking00@hotmail.com, giminiking99@yahoo.com, and hungobject@hotmail.com. On or about February 14, 2022, the Provider responded to the legal service and indicated that the email address hungobject@hotmail.com was associated with the Subject Account**.**

38. A driver's license check on the name Gerardo Montes located an individual with a listed address in Honolulu, Hawaii. Additionally, the record also indicate this Gerardo Montes is 31 years old.

CONCLUSION

39. Based on the forgoing, I request that the Court issue the proposed search warrant. The United States will execute this warrant by serving the warrant on the Provider. Because the warrant will be served on the Provider, who will then compile the requested records at a time

convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

40. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

41. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

I state under the penalty of perjury that the foregoing is true and correct.

Respectfully submitted,

DEREK G. VELAZCO
Special Agent
FEDERAL BUREAU OF INVESTIGATION

Sworn to, attested to, or affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41 on March 9 **, 2022.**

THE HONORABLE NOELLE C. COLLINS
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with Discord account, **HUNGOBJECT#3945 (USER ID 730942504312111125**, that is stored at premises owned, maintained, controlled, or operated by DISCORD, INC., a company headquartered at 444 DE HARO ST., SUITE 200, SAN FRANCISCO, CA 94107.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by DISCORD, INC. (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider. The Provider is required to disclose the following information, for the time period of 01/01/2021 to Present, to the United States for each account or identifier listed in Attachment A:

The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

a. All records or other information regarding the identification and subscriber of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

b. The types of service utilized;

c. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

d. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

e. Any and all cookies associated with or used by any computer or web browser associated with the account, including the IP addresses, dates, and times associated with the recognition of any such cookie;

The Provider is hereby ordered to disclose the above information to the United States within 14 days of the date of this warrant.

II. Information to be seized by the United States

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations Title 18, United States Code, Sections 875(d), 2251, 2252, 2252A, 2261A(2)(b), and/or 2422, those violations involving Gerardo Montes from 01/01/2021 to Present, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) Communications by and between "hungobject" and F.W., including any digital media shared between the two;

(b) The creation, maintenance, receipt, distribution and transportation of child exploitative materials;

(c) Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

(d) Evidence indicating the account owner's state of mind as it relates to the crime under investigation;

(e) The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s).

(f) The identity of the person(s) who communicated with account about matters relating to the creation, maintenance, receipt, distribution and transportation of child exploitative material, including records that help reveal their whereabouts.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by **Discord, Inc.**, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of **Discord, Inc.**. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of **Discord, Inc.,** and they were made by **Discord, Inc.** as a regular practice; and

b. such records were generated by **Discord, Inc.** electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of **Discord, Inc.** in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by **Discord, Inc.**, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date	Signature